

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

WE CLAIM:

1. (currently amended) A method for basis conversion between a pair of correspondents exchanging cryptographic data, said method comprising the steps of:
transmitting an element represented in a first basis from a first correspondent to an intermediate processor;
converting the transmitted element into a second basis representation by said intermediate processor to produce a converted element;
forwarding said converted element to the first correspondent; and
operating on said converted element by said first correspondent in a cryptographic operation to obtain a result of said cryptographic operation for use in exchanging cryptographic data with said second correspondent.
2. (original) A method according to claim 1 further comprising the step of: transmitting a the result of said cryptographic operation to said second correspondent.
3. (original) A method according to claim 2, wherein said result is a signature.
4. (original) A method according to claim 2 further comprising the step of transmitting said converted element by said intermediate processor to said second correspondent.
5. (original) A method according to claim 2 further comprising the step of transmitting said converted element by said first correspondent to said second correspondent.
6. (original) A method according to claims 4 and 5, wherein said converted element is a short term public key.

Appl. No. 09/933,720

Reply to Office action of May 20, 2004

7. (original) A method according to claims 4 and 5, wherein said converted element is a long term public key.
8. (original) A method according to claim 1, wherein one of said correspondents is a low power computing device.
9. (original) A method according to claim 8, wherein said low power computing device is a smartcard.
10. (original) A method according to claim 1, wherein said cryptographic operation employs an elliptic curved scheme.
11. (original) A method according to claim 1, wherein said intermediate processor is a Certifying Authority.
12. (currently amended) A method for information exchange between a pair of correspondents exchanging cryptographic data and operating in different basis, the method comprising the steps of:
 - transmitting an element represented in a first basis from a first correspondent to an intermediate processor;
 - transmitting of a second element represented in a second basis from a second correspondent to said intermediate processor;
 - converting the transmitted first element into said second basis representation by said intermediate processor to produce a first converted element;
 - converting the transmitted second element into a first basis representation by said intermediate processor to produce a second converted element;
 - forwarding said first converted element to said second correspondent; and
 - forwarding said second converted element to said first correspondent.
13. (original) A method according to claim 12 further comprising the step of operating on said second converted element by said first correspondent in a cryptographic operation to produce a result.

Appl. No. 09/933,720

Reply to Office action of May 20, 2004

14. (original) A method according to claim 13 further comprising the step of operating on said first converted element by said second correspondent in said cryptographic operation to produce a second result.
15. (original) A method according to claims 13 and 14, wherein said converted elements are public keys.
16. (original) A method according to claim 15, wherein said result is a common key shared between said correspondents.
17. (original) A method according to claim 16 further comprising the step of employing said common key in subsequent steps of a cryptographic scheme.
18. (original) A method according to claim 17, wherein said cryptographic scheme is an elliptic curve scheme.
19. (original) In a cryptographic system, a method for generating a basis independent bit string, the method comprising the steps of:
representing a first field element in terms of a first basis;
computing a first function of a first sequence of traces of said first field element; and
using said first sequence of traces as said bit string.
20. (original) A method according to claim 19 further comprising the steps of:
representing a second field element in terms of a second basis; computing a second function of a second sequence of traces of said second field element; and
using said second sequence of traces as said bit string.
21. (original) A method according to claim 20, wherein said first function is equal to said second function.
22. (original) A method according to claim 20, wherein an order of said sequence of traces is shared between a first correspondent and a second correspondent.

Appl. No. 09/933,720

Reply to Office action of May 20, 2004

23. (original) A method according to claim 20 further including the step of using said bit string as a shared secret in a cryptographic scheme between a first correspondent and a second correspondent.
24. (original) A method according to claim 23, wherein said cryptographic scheme is an elliptic curved scheme.
25. (original) A method according to claim 19, wherein said first function is an irreducible polynomial of degree N.
26. (original) A method according to claim 20, wherein said second function is an irreducible polynomial of degree N.
27. (original) A method according to claims 24 and 25, wherein said first field element is converted in terms of said second basis by finding a root for said polynomial for said first basis in a representation generated by said second basis; and evaluating said polynomial representing said first field element in said first basis at said root.